Level(3) COMMUNICATIONS
Connecting and Protecting the Networked World℠

Can Technology Save us from Evolving Cybersecurity Threats?

Bruce Roton
CISSP, CISM, CEH, CISA, CGEIT, ISO27001, CSSGB
Director, Security Solutions Architecture, Level 3 Communications

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

Disclaimer:

The purpose of this presentation is solely educational.

The content and opinions contained in this presentation are attributable to me solely in my personal capacity, and are neither endorsed by nor reflect the opinions of my employer, Level 3 Communications.

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

Security services must be integrated with networks to make the network services **More Secure**, **More Functional**, **More Cost Effective**, and **More Convenient** for Businesses and Consumers.

Agenda

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

1. Trends in the Cyber Security Space
2. Examples of Advanced Analytics
3. Security Recommendations

The Past 10 Years of Environmental Evolution

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

Changing Business Models

- Eroded Perimeter
- Employee Mobility
- Cloud-based Services
- BYOD
- Distributed Environments
- 3rd party Software
- Social Networking

Evolving Threat Landscape

- Attacks Are Changing:
- Perpetrators
- Targets
- Form and Complexity
- DDoS (10% to 50+%)
- Sophistication
- Tool sets
- Frequency

Security: Frozen in Time

- Overall, the Security Industry has not advanced to keep pace with the environment

Key Security Trends & Advanced Threats

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

- DDoS Attacks are still the number one attack vector (+54% of attacks)
- Advanced malware threats are the second most common
  - What is an advanced malware threat, and what are the attackers after?
    - Sophisticated data exfiltration software designed to evade detection
    - Financial data, PI (Identity Theft), Healthcare data, and Intellectual Property
  - Why are the attacks so common? Tools, Tools, and more tools
  - How does the malware get into the enterprise?
    - Spear Phishing Attacks
    - Drive By Downloads
    - Watering Hole Attacks

The Attack Event Chain

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

It has been said that defenders have to get it right all the time, while attackers only have to get it right once to succeed. This might have been true in the past, but the nature of today's attacks (profit motivated), require a complex chain of events that must all work for the attack to be successful.

1. Reconnaissance and discovery
2. Attack strategy and exploit development
3. Initial intrusion (establishing a beachhead)
4. Target acquisition (locating the valuables)
5. Creation of an exfiltration path
6. Capture, encryption, and exfiltration.
7. Monetization

- **Scanning**
- **Phishing**
- **Malware download**
- **C2 Comms**

Zero Day Exploits vs. Zero Day Vulnerabilities

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

Attacks Are Changing In Form, Complexity, Volume and Timing

New 0-day Vulnerabilities discovered weekly and sold for $$$$

Over 6 million mobile malware samples collected in Q4, up 14% over Q3.
Source: McAfee Labs Threat Report, Feb 2015

1,800 Number of new distinct families of viruses detected in the past year
Source: Fortinet Threat Landscape Report 2014

Increase in attacks against core infrastructure code: NTP, Heartbleed, Winshock, Shellshock
Source: McAfee Labs Threat Report Q1 February 2015

$3.5M Global average cost to a company due to data breaches and 15% more than it cost in 2013
Source: Ponemon 2014 Cost of Data Breach Study: Global Analysis

160K New samples of malware released everyday
Source: Panda Quarterly Report, 2014

Why Can't We Make it Secure Through Testing?

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

- First and foremost the goal of testing has traditionally been to validate that something works and does what we planned, not to see if we can make it do unplanned stuff.
- Vulnerability assessors and Penetration testers generally don't build custom tools just to exploit your environment.
- VA's and Pen testers do not have the same level of motivation as a hacker.
- VA's and Pen testers care about collateral damage
- VA's and Pen testers don't have years to find your weak spots

Why Security Architectures Fail

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

Two Primary Reasons

SOFTWARE

Developed by humans and not perfect

PEOPLE

Coincidentally, also developed by humans and not perfect

(social engineering works)

Jericho Security Model

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

This model postulates that we cannot protect the network itself, or all of the system elements. The Network perimeter is too porous to defend 100%.

Therefore, we should allow an open network and focus on containment of valuable assets into defensible zones.

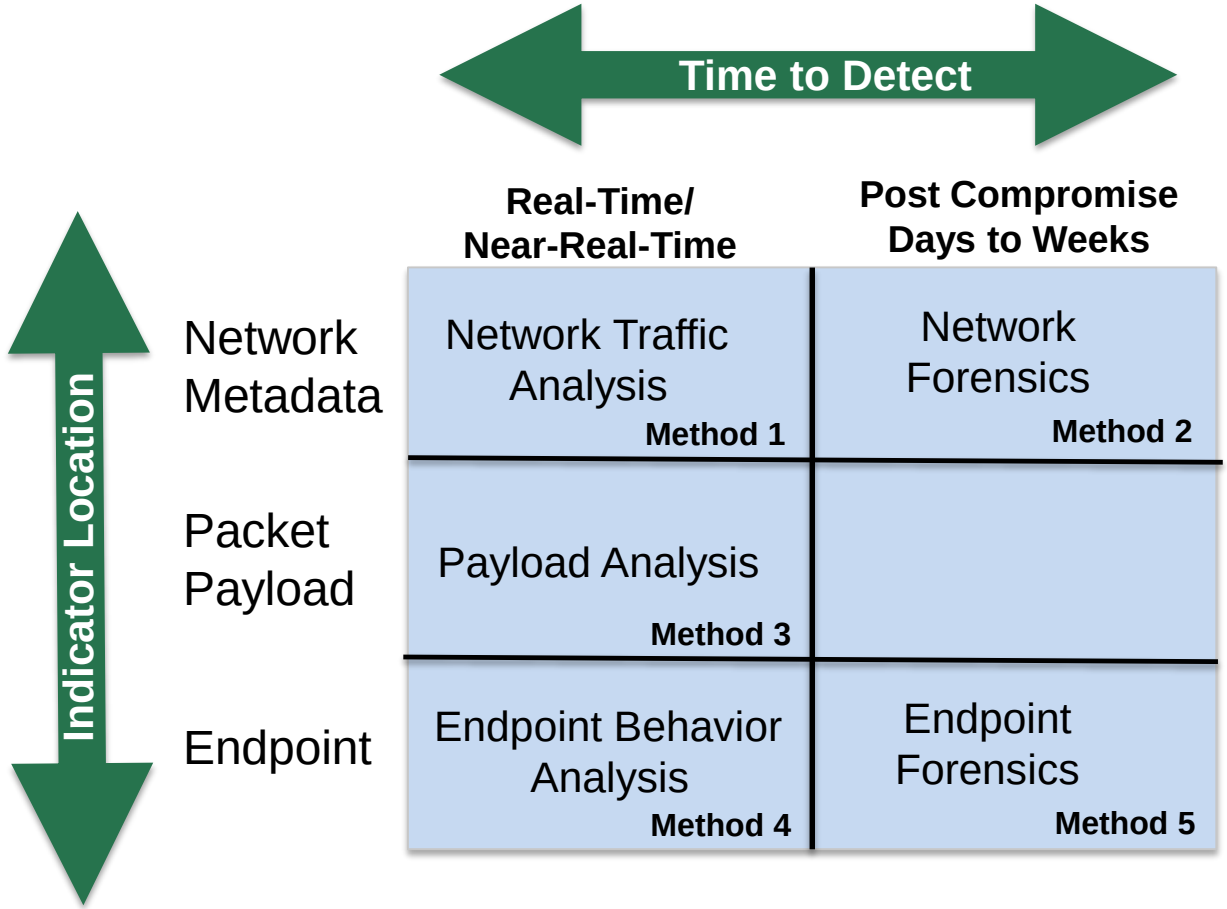
These security zones can then be tightly controlled.

In this model, we focus on the protection of specific assets through:

- Strict Identity Management
- Strict access control
- Comprehensive activity and state monitoring

New “Standards” of Defense

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠



Focus on Mitigation with Methods 1, 3, and 4

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

Payload — This approach typically uses a sandbox (an isolated, simulated environment) to observe the behavior of payloads in motion (as they cross the network perimeter) and to flag those that are suspicious. However, this can also include near real time analysis using payload "rules" based on previous forensic analysis.

Endpoint — This approach provides the most detailed information about how endpoints have been impacted by malware and Advanced Technical Attacks, but it comes with the operational cost of implementing and managing agent software on every endpoint. It may also be detected and evaded by the malware.

Network — By analyzing inbound and outbound network traffic, this technique can identify potentially compromised endpoints. Further, such systems may detect and block attacks in real time.

Payload Analysis

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

- **Payload capture and analytic modeling**
  - PCAP and reassembly or redirection to sandbox virtual host
- **Two triggers for evaluation**
  - **Fingerprinting:** Size of the malware payload, Executables and scripts, Application and port targeting
  - **Behavioral:** Analysis of sandboxed malware behavior
- **Data Mining for Payload Signatures**
  - Step 1: Use honeypots/tar-pits to attract and capture
  - Step 2: Lots of post attack traffic correlation to identified attacks
  - Step 4: Reverse engineer captured malware to determine purpose and look for similar activities
  - Step 5: Build a behavioral database and heuristics engine to automatically generate new rules
- AhnLab, FireEye, Lastline, McAfee (ValidEdge), ThreatGrid

Endpoint Behavioral Analysis

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

Three Types of Solutions

- **Application Containment:** Blue Ridge, Bromium, Invincea, Sandboxie, Trustware
- **Memory Monitoring:** Cyvera, ManTech/HBGary, RSA, Mandiant*
- **System Configuration and Process Monitoring:** Triumfant

Application containment protects endpoints by isolating applications and files in virtual containers. Allows malware to execute, but it does so in a sandbox so all access to content and information outside of its container is controlled and monitored.

Memory monitoring detects attacks by examining the behavior of memory resident software.

Configuration and Process monitoring controls changes to system configurations and acceptable process operation.

Downside: These solutions require an agent on every endpoint.

Network Analytics Using Netflow

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

- **Catches the obvious**
  - Abuse (iTunes and web-radio) and Misuse (P2P and Gaming)
- **Catches the less obvious**
  - Communications to restricted or suspicious locations
  - Unexpected/Banned protocols and Encrypted channels
- **Can catch the true outliers (a bit more work/storage)**
  - Rare Communications and slow but regular communications
  - New behaviors and connections
- **Potential triggers and fingerprinting**
  - Packet size within sequence: fingerprint potential malware download
  - Conversation timing: Associating packet delta with specific malware
  - Flags and window size: Fingerprinting systems and malware
- **Data Mining for Traffic Signatures**

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

Example of Enterprise Protection

Global Security Scope of Operation

Level 3 operates some of the worlds largest networks and application environments

- Level 3 Global Internet
  - 11 Tbps of traffic continuous
- Level 3 DNS Caching Infrastructure
  - http://en.wikipedia.org/wiki/User:Incu_Master/4.2.2.2
- Level 3 CDN

Global Security Monitoring Environment

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

THE LEVEL 3 GLOBAL SECURITY OPERATIONS CENTER (SOC) MONITORS:

1000	1+ MILLION	1.3 Billion	Tracking Nearly 3 million	45+ Billion
Command and Control Servers	Malicious Packets Per Day	Security Events Per Day	Compromised Computers Each Day	Netflow Sessions Per Day

Level 3 monitors 950 million security events per day (Enterprise, Products, Managed Security**)**

- **Level 3 monitors over 45 billion netflow sessions per day (**Over 2.5 TB per day)

Level 3 performs daily audits, protect and monitor all Level 3 products, services and systems

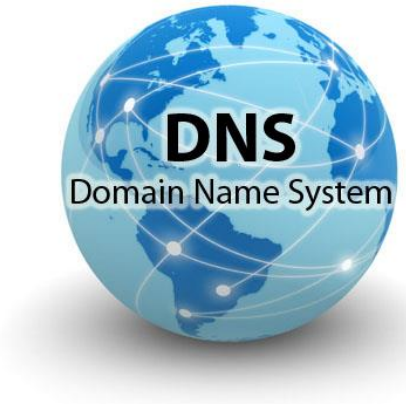
- 200,000 elements (130k network, 70k systems)

Data Analytics in DNS

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

Leveraging Data Analytics on DNS data to identify C2 servers, Attack Campaigns, and Malware Distributors

- Botnets and other malicious software use domain names to communicate ,
- Static IP and DNS blacklists have limited effectiveness as attackers frequently switch to different domains

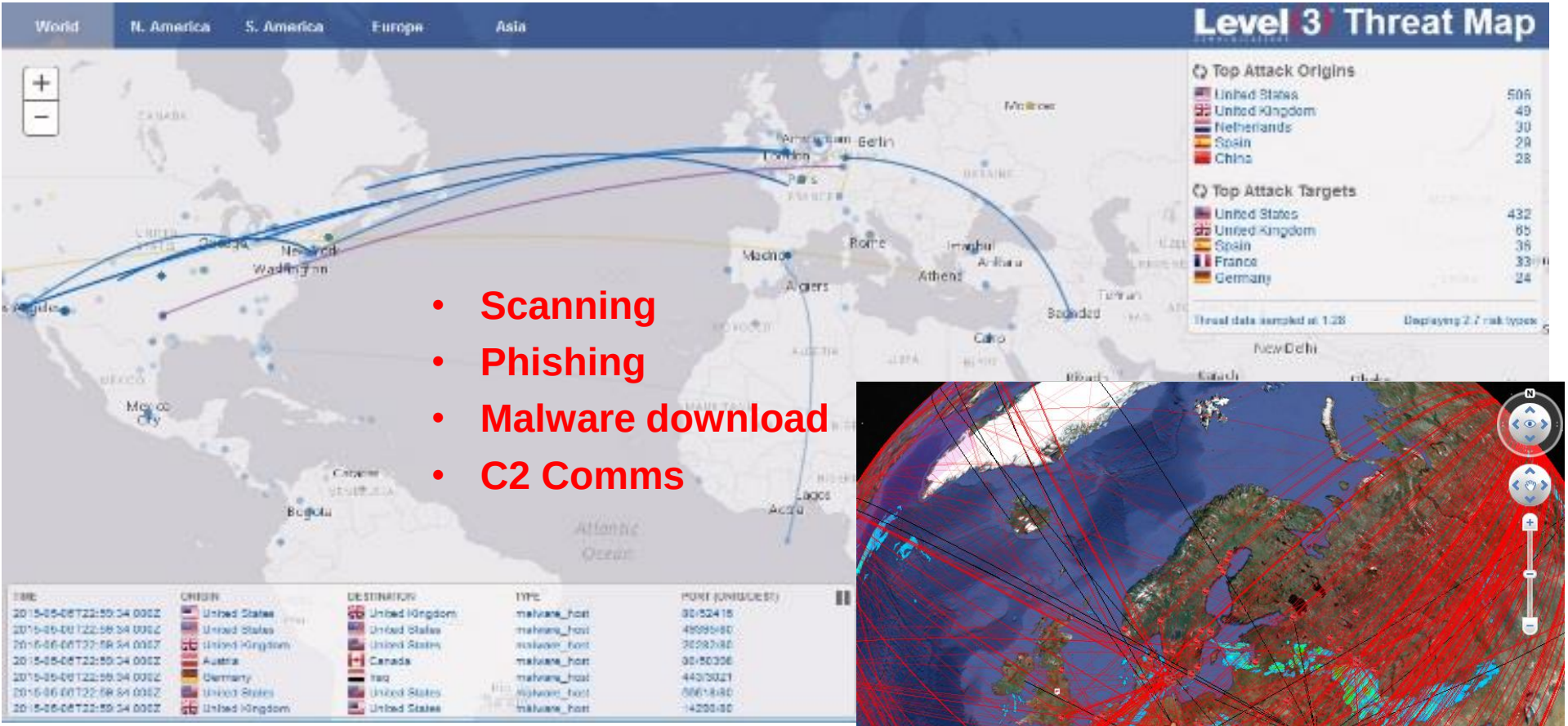


<u>Multiple Approaches to identify Malware related domains</u>:

- Monitor streams of DNS queries and response patterns to detect Malware domain names
- Identify Fast-flux domains - Malware related domains tend to have a short TTL with constantly changing destination IP addresses for a single DNS domain name
- Track create dates and domain history
- Track associated IP range ownership over time.

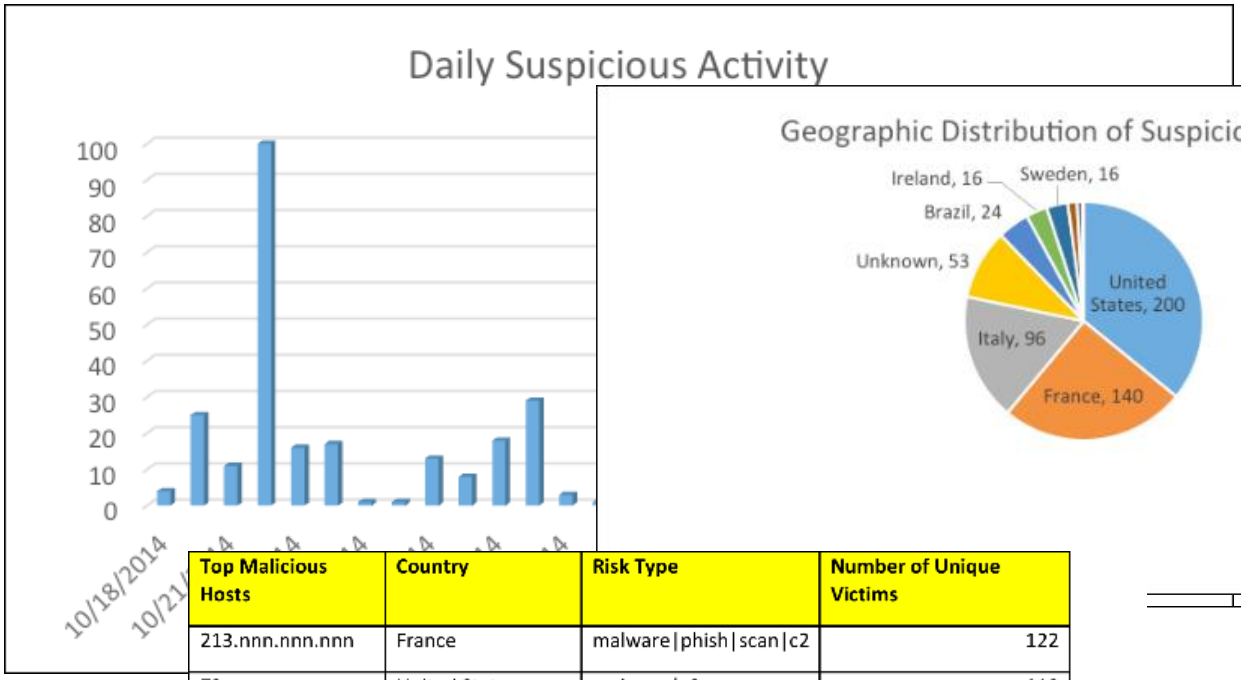
Level 3 Next Generation Threat Intelligence

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

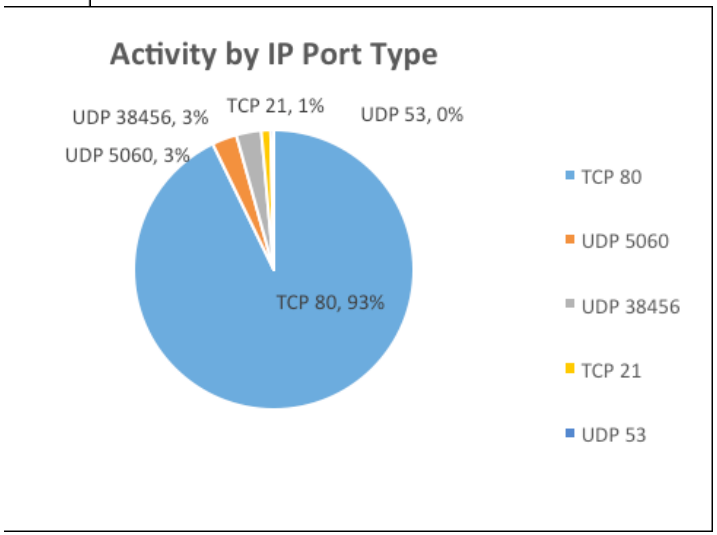


Threat Intelligence Must Be Actionable

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠



Top Malicious Hosts	Country	Risk Type	Number of Unique Victims
213.nnn.nnn.nnn	France	malware|phish|scan|c2	122
72. nnn.nnn.nnn	United States	malware|c2	119
81. nnn.nnn.nnn	Italy	malware|scan|c2|phish	96
66. nnn.nnn.nnn	United States	malware|c2	42
208. nnn.nnn.nnn	United States	malware|c2	35
187. nnn.nnn.nnn	Brazil	malware|c2	23
185. nnn.nnn.nnn	Ireland	malware|scan|c2	19
193. nnn.nnn.nnn	Sweden	malware|c2	16
104. nnn.nnn.nnn	United States	malware|c2	14
104. nnn.nnn.nnn	United States	malware|c2	13



Source: Level 3 Communications, Jan 2015

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

Recommendations

Best served in the Cloud, Leave it in the Cloud

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

Secure Connectivity Solutions

- Site-to-Site tunnels
- Remote user connection solutions
- Mobile Device Management
- Carrier Cloud Based Solutions such as WAN to Internet connectivity

DDoS Protection

- Distributed infrastructure for built-in scalability, redundancy and resilience
- Premises Based Mitigation Will Not Work

Cloud Based Web/eMail Protection

- Distributed infrastructure for built-in scalability, redundancy, resilience, and mobile support
- No premises hardware or maintenance costs
- All the functions and features of a premises based solution

Additional Recommendations

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

- **Focus on the easy stuff first and harness the power of your network visibility and controls (Detective/Preventive)**

Excuse me, but what are you looking for?

- **Define suspicious, and then look for it!**
  - **Where is Data-XXX supposed to live and have you seen it anywhere else?**
  - **Inspect new outbound blocking for IOC**
  - **Should that server ever communicate with anyone outside this network?**
  - **Exactly who should be accessing those data stores?**
  - **Should Fill in the blank type of data be traversing your network?**
  - **Do you have a business partner in Iran?**
  - **Should that comms channel really be encrypted?**
  - **Why is there a Telnet session running or port 25?**
  - **Consider Domain ages (are you old enough to be talking to me?)**

The Criticality of an Information Security Management System (ISMS)

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

- **Defining an InfoSec Management Program and making it work.**
  - **Pick a Standard Framework (ISO27001, NIST-800, PCI, etc…)**
  - **Senior Management buy in is essential**
  - **Allocate resources and fund the program (or fail)**
  - **Define the goals, objectives, and charter (AKA Policy Statement)**
  - **Data Classification and Valuation first, then Discovery.**
  - **Identify your practice areas and assess your maturity (CCM).**
  - **Create practice area targets based on Risk, and create a remediation roadmap clearly linked to the practice area targets.**
  - **Define process for monitoring, measuring and reporting on progress**
  - **Now you can start controls remediation!!!**

Summary – Key Observations

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

- The threat landscape is evolving rapidly due to nation-state, organized crime, and cyber terrorism
- Organizations must assume the "new normal" -- at least some parts of their networks have been compromised
- Your data is an asset – *and a potential liability* -- understand its value, location, and movement
- Perform regular security evaluations, risk assessments, and awareness training for employees
- Determine core competencies, perform functions that you do well, outsource others to trusted, skilled firms
- Some security functions must be done in partnership with your service provider(s)
- Information sharing partnerships are essential, e.g. Infrgard
- Technology is important, but it's not a "cybersecurity panacea"
- Utilize threat intelligence, but in a distilled, actionable form